iDIRECT Government

RESILIENT. SECURE. INNOVATIVE.

Security Content Automation Protocol (SCAP)

iDirect Government is dedicated to guarding our customer networks against security threats. To do so, we utilize security content automation protocol (SCAP) standards to decrease and manage the vulnerability of deployed systems.

What is SCAP?

Defense (DoD) Information Assurance (IA), and IA-enabled devices and systems.

Since 1998, the Defense Information Systems Agency (DISA) Field Security Operations (FSO) has played a critical role enhancing the DoD's security systems by providing SCAPs, which contain technical guidance to "lock down" information systems and software that might otherwise be vulnerable to a malicious computer attack.

iDirect Government's implementation of SCAP standards is the most up-to-date to ensure the highest level of compliance has been met. In addition, we support a number of manual configuration changes to meet additional SCAP guidelines, including Red Hat Linux-specific recommendations, including security concerns ie. Drovorub*.

Security Readiness Review (SRR) scripts test products for SCAP compliance and are available for operating systems and databases that have SCAPs.

Information Assurance Requirements

IA is becoming a very critical component of any organization's information systems management strategy to ensure data and systems' integrity, confidentiality and availability are protected and available to support the missions at hand. Threats to systems and data come in many forms ranging from malware infecting a system to a sophisticated cyber-attack on critical systems by state-sponsored actors. Cyber-attacks have become so sophisticated and serious that governments have devoted entire organizations specializing in counter cyber intelligence to combat this problem around the clock.

iDirect Government provides the following SCAP support:

- Two SCAP packages delivered annually to Premium iSupport customers via the iDirect Government TAC website
- Covers NMS server, PP server, GKD server and Host O/S
- Offered on current Major Defense-Based Release* and one Major Defense-Based Release prior

**Red Hat Linux 8 support beginning with Evolution Defense 4.4*

**Must be operating on Evolution Defense 4.4 to address security concerns associated with Drovorub.*